AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for establishing a secure communications session between a ~~calling party~~first computing device and a ~~called party~~second computing device, ~~consisting essentially~~ the method comprising ~~of~~:

~~identifying~~ retrieving a first ~~shared~~ random number ~~associated with a called party~~at the first computing device;

~~identifying~~ retrieving a second ~~shared~~ random number ~~associated with a calling party~~at the second computing device;

~~said called party generating~~retrieving- at least one public-private key pair including a public key and a private key;

~~transmitting~~ sending a ~~first~~ message from said ~~called party~~second computing device to said ~~calling party~~first computing device, said ~~first~~ message from said second computing device to said first computing device including said first ~~shared~~ random number and ~~said~~ the public key of said at least one public-private key pair to thereby share at least said first random number with said first communication device, said ~~first~~ message from said second computing device to said first computing device being ~~encoded~~ encrypted with an encoded ~~symmetric encryption key~~password;

providing said encoded password to said first computing device;

using said provided encoded password to decrypt said first message at said first computing device to obtain at least said first random number that said second computing device sent in said message from said second computing device to said first computing device;

~~transmitting~~ sending a ~~second~~ message from said ~~calling party~~first computing device to said ~~called party~~second computing device, said ~~second~~ message from said first computing device to said second computing device including said second ~~shared~~ random number, said ~~second~~ first computing device encrypting said message ~~being encoded~~ it sends to said second computing device~~with said public key of said public-private key pair~~; ~~and~~

generating, at each of said first and second computing devices, ~~obtaining~~ a shared ~~secret~~ session key ~~from an output of a combining function having a first input including~~by combining said first ~~shared~~ random number and ~~having a second input including said~~ second ~~shared~~ random number that is now available to each of said first and second computing devices through said above-mentioned message exchanges; and

using said shared session key to establish a secure private communication session between said first and second computing devices.~~.~~

2. (Currently amended.) The method of claim 1, wherein said combining ~~function~~ includes a logical function.

3. (Previously Presented.) The method of claim 2, wherein said logical function includes an exclusive or (XOR) function.

4. (Cancelled.)

5. (Cancelled.)

6. (Cancelled)

7. (Cancelled.)

8. (Cancelled)

9. (Cancelled.)

10.–153. (Cancelled.)

154 (Currently amended). A method for establishing secure communication between a calling party and a called party, comprising:

generating, on demand at the called party, an asymmetric key pair including a public key and a private key;

transmitting, from said called party to said calling party, a first encrypted message including a first random number and said public key of said asymmetric key pair, said called party encrypting said first message with an encoded password ~~symmetric encryption key~~ known to both the calling party and the called party;

said calling party receiving and decrypting said first encrypted message using said ~~symmetric encryption key~~encoded password to obtain said first random number and said public key;

said calling party transmitting, to said called party, a second encrypted message including a second random number, said calling party encrypting said second message with said public key of said asymmetric key pair;

said called party receiving and decrypting said second encrypted message to obtain said second random number;

said calling and called parties each independently applying said now-shared first and second random numbers to combining functions to thereby each independently generate a shared secret key; and said calling and called parties encrypting further communications therebetween at least in part using said shared secret key.

155 (Previously presented). The method of claim 154 wherein said symmetric encryption key comprises a password.

156 (New). The method of claim 1 wherein said password comprises a user password.

157 (New). The method of claim 1 wherein said encoded password comprises a user password encoded with a hash function.

158 (New). The method of claim 1 further including generating said first and second random numbers on demand.

159 (New). The method of claim 1 further including generating said public-private key pair on demand.

160 (New). The method of claim 1 wherein said second computing device comprises a server, and said first computing device comprises a client wishing to communicate with said server.

161 (New). The method of claim 1 wherein said first computing device uses said public key obtained from said message send from said second computing device to said first computing device to encrypt said message from said first computing device to said second computing device.

162 (New). The method of claim 1 further including prompting a user to input a password into said first computing device, and encoding said inputted password at said first computing device to provide said encoded password.

163 (New). The method of claim 154 wherein said called party comprises a server and said calling party comprises a client that wishes to communicate with said server.

164 (New). The method of claim 154 further including said called party retrieving said password or encoded password from a user database in response to receipt of a request by said calling party for a secure communication.

165 (New). The method of claim 154 wherein said generating comprises generating said asymmetric key pair at said called party.

166 (New). The method of claim 154 wherein said encrypted communication proceeds between said calling party and said called party without requiring said calling party to generate an asymmetric key pair.